Communiqués et discours

Discours

ALLOCUTION DE LA PRÉSIDENTE DE LA COMMISSION D'ACCÈS À L'INFORMATION, MADAME JENNIFER STODDART,
À LA 17e ÉDITION DU CONGRÈS
MONTRÉAL 2002 IFIP WORLD COMPUTER CONGRESS
GOUVERNEMENT EN LIGNE ET RESPECT DE LA VIE PRIVÉE : UN DÉFI DE TAILLE

Le 27 août 2002

INTRODUCTION

L'avènement du gouvernement électronique, ici comme ailleurs dans le monde, peut avoir des avantages réels pour les citoyens. En principe, le e-gouvernement devrait permettre une plus grande participation des citoyens dans la vie publique et dans la gestion de leur société, sans parler de la vitesse et de la précision avec lesquelles des services gouvernementaux pourraient être rendus. Il devrait permettre une distribution de services plus juste et plus ciblée, appuyée sur une information qui se modifie très rapidement au gré de la cueillette des données auprès des usagers. La réduction de l'intervention bureaucratique dans les transactions des citoyens avec le gouvernement devrait, de plus, minimiser les fléaux qui guettent toute administration publique : l'exercice arbitraire du pouvoir discrétionnaire et la discrimination.

Voilà de bonnes raisons qui stimulent les administrations publiques à travers l'Occident, à proposer des projets, de plus en plus englobant, pour le gouvernement en ligne.

Mais comme on le sait, ces projets peuvent comporter des risques réels pour la vie privée, voire mener à des pertes irrémédiables du niveau de protection de la vie privée à laquelle on est habitué.

C'est pourquoi l'organisme comme celui que je préside a notamment comme mandats la surveillance et le contrôle, par des avis, des projets potentiels de gouvernement en ligne.

Dans les propos qui suivront, je veux d'abord identifier les fonctions de l'organisme que je dirige pour ensuite proposer une série de critères que nous utilisons pour l'évaluation de projets. Je terminerai avec l'exemple de quelques-uns des projets récents que nous avons été appelés à évaluer pour illustrer concrètement l'application des préoccupations de la Commission d'accès à l'information concernant la vie privée.

2008-05717/

L'ACCÈS À L'INFORMATION ET LA DÉMOCRATIE

Comme nous l'avons tous déj à entendu : le savoir c'est le pouvoir. Depuis l'avènement des nouvelles technologies de l'information, le savoir est à la portée de tous les citoyens. L'accès à une plus grande source d'information est garant de la vie démocratique de tous les peuples. Au cours des 30 dernières années du 20ième siècle, nous avons été témoins d'une tendance au partage de l'information jusqu'alors détenu par les démocraties et guère disponible au public.

Ainsi, aux États-Unis, une longue tradition de démocratisation associé à un manque de confiance historique des pouvoirs étatiques a amené l'adoption de la législation intitulé : the *Freedom of Information Act in 1974*(1). En même temps, la préoccupation de l'accès à l'information détenu par les états notamment de l'Union Européenne, du Canada et particulièrement du Québec n'a fait qu'augmenter. Le Québec est une province de la fédération canadienne qui se démarque par une culture distincte. Il y a au Québec une législation également distincte en matière d'accès à l'information dans sa compétence propre.

Au début des années 80 une commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels soulignait le fait suivant : « Sans avoir accès aux faits, sans information, la liberté d'opinion est vidée de substance. Le savoir conditionne l'exercice du droit d'expression La puissance des techniques de communication contemporaines et le large recours de l'État à ces techniques conduisent facilement à la propagande qu'il est impossible aux citoyens, aux associations et même aux entreprises de presse les mieux organisées et les mieux pourvues de contrer. » (2)

LES MANDATS ET FONCTIONS DE LA COMMISSION D'ACCÈS À L'INFORMATION

La Commission d'accès à l'information voit à l'application de deux lois : la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé.*

Secteur public

Dans le secteur public, ministères, organismes gouvernementaux, municipalités, institutions d'enseignement, ainsi que les établissements du réseau de la santé et des services sociaux sont assujettis à la Loi sur l'accès qui comporte deux volets. Le premier garantit à toute personne un droit d'accès aux documents des organismes publics. Le second volet est destiné à assurer une protection maximale des renseignements personnels que détient l'administration publique. Ce second volet de la loi reconnaît aussi à chaque citoyen un droit d'accès et un droit de rectification de ses renseignements personnels.

Secteur privé

Dans le secteur privé lors de l'application de la *Loi sur la protection des renseignements personnels* prévoit que toute entreprise de biens et services doit se conformer à celle-ci dès l'instant où elle recueille, détient, utilise ou communique des renseignements personnels. Afin d'assurer le contrôle des renseignements le concernant, tout individu dispose d'un droit de regard sur son dossier, notamment par le droit d'accès et le droit de rectification, ainsi que le droit de faire retrancher d'une liste nominative tout

renseignement détenu ou utilisé par une entreprise à des fins de prospection commerciale ou philanthropique.

Fonction d'adjudication

En tant que tribunal administratif, la Commission révise les décisions des administrations publiques à la suite de demandes provenant de personnes à qui on a refusé, soit l'accès à un document administratif, soit l'accès ou la rectification de leur dossier personnel. Elle est aussi appelée à trancher les mésententes découlant de l'exercice des droits reconnus par la Loi sur le secteur privé.

La Commission tente d'abord d'obtenir un règlement de ces litiges par voie de médiation. En cas d'échec, elle permet aux parties de présenter des observations sous forme écrite ou verbale et rend une décision. Cette décision est finale sur les questions de faits; les questions de droit ou de compétence peuvent être portées en appel devant la Cour du Québec, avec permission d'un juge de cette cour.

La fonction de surveillance et de contrôle

La Commission a aussi comme mandat de veiller au respect des obligations imposées aux organismes publics et entreprises privées en matière de collecte, de détention, d'utilisation et de communication de renseignements personnels. è cette fin, elle peut être appelée à autoriser les chercheurs à recevoir des renseignements, à donner des avis sur des ententes de communication de renseignements personnels, à mener des enquêtes, de sa propre initiative ou à la suite d'une plainte, à procéder à des vérifications du respect des lois et à formuler des avis sur des projets de loi ou de règlement dont les dispositions peuvent avoir un impact sur les normes établies.

La fonction de conseil

La Commission s'est enfin donné pour objectif de faciliter l'implantation de mesures concrètes qui permettent de respecter l'esprit et la lettre de la loi. C'est à ce moment qu'intervient la Commission pour conseiller les organismes publics et privés. Cette fonction stratégique de la Commission se manifeste de différentes façons : lignes politiques et évaluation de projets pilotes touchant notamment des dossiers de haute importance comme les nouvelles technologies de l'information, la génétique, la biométrie, etc. Dans le cadre de cette fonction, la Commission participe à des conférences et des colloques.

MOYENS POUR GARANTIR LE RESPECT DE LA VIE PRIVÉE

Au moment d'écrire ces lignes, le gouvernement Japonais fait face à une farouche opposition de la part de sa population et de nombreuses autorités municipales[3]. La source de ce conflit est la mise en service récente d'un système national d'identification appelé Juki Net qui permet aux administrations locales d'identifier en ligne chaque citoyen Japonais. Pour ce faire un numéro unique à 11 chiffres est attribué à chaque personne.

Si les opposants à ce système se font quelques soucis en raison de son possible piratage, leurs principales inquiétudes concernent les menaces que font peser ce projet sur leur vie privée; Juki Net est considéré par plusieurs comme un système de surveillance de la population[4]. Plusieurs autorités locales ont refusé de se relier au

système pendant que d'autres, comme à Yokohama seconde ville du Japon[5], décidaient d'enregistrer seulement les personnes qui en exprimeront le souhait.

Le maire de la ville de Kokubunji a même organisé une séance de déconnexion à l'hôtel de ville et un autre maire d'une ville située au nord de Tokyo déclare que « Juki Net était très risqué car une loi sur la protection des informations personnelles était toujours en attente au Parlement. »

En effet, en 1999 lorsque le gouvernement Japonais lançait l'idée de ce système, il promettait l'adoption préalable d'une loi sur la protection des informations personnelles.[6] La législation est le premier outil de protection de la vie privée et ce bien avant tout outil technologique de sécurité. Mais cet outil n'a de sens que s'il prend racine dans la culture et les valeurs d'une société. L'exemple japonais l'illustre fort bien. Malgré les garanties des autorités nationales que le système est pleinement sécuritaire,[7] la contestation est vigoureuse. De nombreux citoyens Japonais réclament l'adoption d'une loi de protection des données personnelles, non pas pour demander une meilleure sécurité des données utilisées par l'État, mais dans le but de protéger leur vie privée.

La passion entourant les actions des opposants au système démontre l'attachement d'au moins une partie de la population envers cette valeur fondamentale de vie privée et l'avenir nous dira si toute la société japonaise y adhère.

En fait de nombreux États ont adopté au cours des dernières années des législations qui assurent la protection de la vie privée ou des données personnelles de leurs citoyens. Si les lois sont différentes d'un pays à l'autre les règles qu'elles proposent sont semblables et portent notamment sur la cueillette, la conservation, la finalité, l'utilisation, la communication des renseignements personnels et leur accès par la personne concernée.

L'expérience de la Commission sur le terrain nous démontre que de nombreux informaticiens, du moins au Québec, confondent confidentialité et protection de la vie privée. La confidentialité est un objectif de sécurité au même titre que la disponibilité et l'intégrité.

Si celle-ci concourt à la protection de la vie privée, elle ne peut permettre à elle seule de l'assurer. Cette assurance provient plutôt de l'application de l'ensemble des règles élaborées dans les lois. L'exemple qui suit devrait vous permettre de bien saisir ce que je veux dire.

Système de santé québécois

La Commission a étudié récemment un système dans le domaine de la santé qui permet la communication de données cliniques entre plusieurs établissements procurant des soins de courte durée à des patients ambulatoires. Ainsi, un patient devant recevoir des soins de plusieurs établissements est assuré qu'un dossier électronique contenant les renseignements nécessaires à ses traitements est rendu disponible aux intervenants de chaque établissement qu'il doit visiter. Les promoteurs du projet ont conçu une architecture basée sur un logiciel permettant la réplication de données. Plusieurs mécanismes de sécurité ont été mis en place. è première vue la loi semblait respectée. Cependant un examen plus poussé du fonctionnement du système nous a laissé voir que celui-ci réplique les données de tous les patients dans tous les établissements qui l'utilisent. Ainsi le dossier d'un patient se trouvait dans les bases de données des établissements qui lui prodiguaient des soins, mais aussi dans les bases de

données des établissements qu'il n'aurait pas à visiter.

La Commission a déterminé, dans ce cas, que les établissements qui ne prodiguent pas de soins à un patient ne peuvent conserver son dossier. Ceci démontre qu'un système sécurisé dans lequel la confidentialité est assurée peut transgresser des règles de protection des renseignements personnels.

Pourtant, tout système mis en service et toute technologie utilisée doivent permettre de respecter les lois qui s'appliquent le cas échéant. Encore une fois, l'expérience sur le terrain nous démontre que dans plusieurs cas les responsables de développements majeurs ont de la difficulté à transposer les règles de protection des renseignements personnels dans le fonctionnement de leurs systèmes. Bien souvent cette considération n'est pas suffisamment approfondie dans les phases préliminaires de développement ou lors de l'acquisition d'une technologie ou d'un système, l'emphase étant mise sur les coûts et les échéanciers.

Ceci à des conséquences néfastes. Imaginez la situation inconfortable dans laquelle se trouveraient les responsables d'un système qui ne respecterait pas la loi, alors que des contrats importants auraient été signés ou que des logiciels coûteux auraient été acquis. Pour éviter de telles situations les projets de ce genre doivent être soumis à une rigoureuse analyse des impacts de l'introduction d'une technologie ou d'un système sur la vie privée des citoyens ou des personnes qui les utiliseront.

La décision de réaliser le projet ou non ne devrait être prise qu'après la réalisation d'une telle analyse. Celle-ci devrait porter sur le potentiel du projet à respecter la vie privée ou la protection des données personnelles tel que requis par les lois et devrait de par surcroît explorer les avenues suivantes. Ces avenues doivent être considérées comme des critères propres à rehausser considérablement le niveau de protection accordé à la vie privée :

- Critère 1
  Favoriser l'anonymat des utilisateurs.

- Critère 2
  Lorsque l'anonymat est impossible à utiliser, favoriser la pseudonymisation.

- Critère 3
  Éviter la cueillette de données personnelles supplémentaires aux seules fins de sécurité.

- Critère 4
  Respecter le cloisonnement administratif entre les différents organismes.

- Critère 5
  Éviter la centralisation et la concentration des traitements et des données.

- Critère 6
  Éviter la dissémination, la duplication, la réplication et le partage des renseignements personnels.

- Critère 7
  Favoriser les technologies qui évitent le traçage des actions des utilisateurs et la constitution de profils.

- Critère 8
  Envisager des moyens de sécurité équilibrés qui permettent d'atteindre les objectifs de sécurité requis tout en respectant la vie privée.

Malheureusement, des méthodes permettant ce type d'analyse ne sont pas légion. Le gouvernement pourrait-il jouer un rôle à cet égard? Devrait-il exiger l'utilisation de tels outils et devrait-il en favoriser l'éclosion?

E-GOUVERNEMENT

Avant de répondre à ces questions, il convient d'exposer certains enjeux qui permettront plus d'acuité dans la réflexion que je ferai par la suite.

Tout d'abord, la difficulté pour un citoyen de comprendre ce qu'il advient de ses renseignements personnels dans un monde virtuel.

Ensuite la quasi impossibilité pour le citoyen de comprendre, de démontrer et de prouver la logique d'une communication illégale ou d'une fuite de renseignements personnels dans un tel environnement.

Enfin la possibilité grandissante qu'un citoyen ne sache jamais qu'il a été victime d'une communication illégale ou d'une fuite de renseignements.

Au printemps 2002, la Commission d'accès fut conviée à déposer un mémoire concernant l'Avant-projet de loi sur la carte santé du Québec devant une Commission parlementaire. Le texte législatif, produit par la Régie de l'assurance maladie du Québec, devait permettre notamment l'instauration d'un système en ligne de vérification de la couverture d'assurance d'un patient, la confection d'un dossier de santé partageable et l'utilisation d'une carte à microprocesseur. Sans l'analyser dans ses moindres détails, je soumets à votre attention au passage, que ce projet ne permettait pas de respecter un des critères aptes à rehausser le niveau de protection accordé à la vie privée que j'ai énoncé un peu plus tôt. En effet le *critère 5* commande d'éviter la centralisation et la concentration des traitements et des données, alors que ce projet fait exactement l'inverse. Mais l à où le bét blesse davantage, c'est que j'ai constaté lors des auditions en Commission parlementaire, que plusieurs experts avaient de la difficulté à cerner le fonctionnement du système proposé et par conséquent de dégager les effets positifs et négatifs dus à son utilisation. Si des observateurs privilégiés éprouvaient de tels problèmes, je vous laisse imaginer ce qu'il en serait pour le citoyen. Comment favoriser un sain exercice de la démocratie dans un contexte où de nombreuses personnes ne sont pas en mesure de comprendre l'essence des changements fondamentaux qui nous sont proposés ?

Un gouvernement peut décider de légiférer pour protéger la vie privée de ses citoyens ou leur laisser le soin de le faire eux-mêmes. Je ne crois pas que cette dernière approche soit suffisante lorsqu'il qu'une société est confrontée à des changements technologiques majeurs dont plusieurs risquent d'avoir des impacts sur la vie privée des citoyens, alors que ceux-ci ne sont pas en mesure d'en comprendre le fonctionnement et ses effets.

Comme nous l'avons vu beaucoup de gouvernements ont fait leurs devoirs en matière de législation répondant ainsi aux désirs et aux aspirations de leurs citoyens. Pourtant de nombreux sondages démontrent que la population demeure inquiète en ce qui concerne la protection de la vie privée lorsque des technologies comme le réseau

Internet est en cause.

De façon générale un gouvernement lorsqu'il légifère doit le faire dans le souci de protéger le citoyen qui lui n'est pas en mesure de comprendre le fonctionnement des systèmes complexes dans lesquels résident ses données personnelles. Il doit aussi s'assurer que le citoyen qui possède des droits puisse les exercer en cas de communication illégale, de fuites de renseignements personnels ou d'autres situations où il est lésé. De plus, un gouvernement ne doit pas hésiter à soumettre les projets qu'il promeut à de véritables débats publics.

Le gouvernement lui-même dans la prestation de services électroniques qu'il offre doit être exemplaire en matière de protection de la vie privée. Pour ce faire, il doit exiger que les ministères et organismes gouvernementaux sous sa responsabilité respectent scrupuleusement la lettre et l'esprit de la loi.

La Commission d'accès a récemment donné son avis sur un projet gouvernemental d'infrastructure à clés publiques (PKI-Public Key Infrastructure); il est à noter qu'il s'agit d'un projet intérimaire et qu'une solution permanente est en cours d'élaboration. Ce projet nécessite des corrections et des améliorations afin que la loi soit respectée. Mais même lorsque que Se sera fait, des irritants pourraient subsister au regard du respect de la vie privée. Mentionnons à titre d'exemple l'obligation pour un utilisateur de décliner de son identité devant un agent vérificateur, une personne externe à l'organisation gouvernementale. Ce choix administratif, sans considérer les autres aspects du projet, entre à lui seul en contradiction avec plusieurs des critères aptes à rehausser le niveau de protection accordé à la vie privée. Tout d'abord il y a contradiction avec le *critère 1*; l'identification formelle, de par sa nature, est l'antithèse de l'anonymat. Puis, des données personnelles supplémentaires étant recueillies par un tiers à des fins de sécurité, le *critère 3* est compromis. Enfin, en disséminant les données d'identification concernant des personnes et en les répétant en plusieurs endroits, le *critère 6* n'est pas respecté.

Ainsi, en ce qui concerne ce projet, il sera peut-être possible à ceux qui en sont à l'origine de respecter la lettre de la loi, mais plus difficilement son esprit qui commanderait de restreindre au minimum la cueillette et la circulation de données personnelles.

Un gouvernement devrait toujours choisir les technologies matérielles et logicielles les moins invasives pour la vie privée des citoyens et de ses employés. C'est pourquoi chaque projet gouvernemental devrait çtre soumis à une analyse rigoureuse des impacts qu'il génère sur la vie privée ou sur la protection des données personnelles des citoyens et sur celle des personnes qui auront à travailler avec le système et la technologie envisagée. Comme je l'ai déj à mentionné, les méthodes d'analyse en cette matière sont plutôt rares.

Un gouvernement pourrait certes développer ou contribuer au développement de telles méthodes. Elles devraient être basées sur des modèles internationaux éprouvés, comme par exemple les Critères Communs, tout en étant assez souple pour tenir compte des différences qui existent d'un État à l'autre dans les législations protégeant la vie privée ou les données personnelles.

Le type d'analyse ici proposé est fort important. Actuellement les États acquièrent à grands frais des logiciels pour lesquels ils ne possèdent pas les sources. Bien souvent le fonctionnement exact de tels logiciels n'est connu que des propriétaires du produit. Ces programmes traitent et manipulent un nombre considérable de données personnelles. Un expert du Centre de bioéthique de l'Institut de recherches cliniques de Montréal

écrivait récemment dans Le Devoir[8]: « En effet, la vérité de la loi (et la suprématie du droit) repose notamment sur le principe selon lequel *nul n'est censé ignorer la loi.* Le gouvernement qui édicte un règlement d'application d'une loi est censé la connaître Mais qu'en est-il du système informatique? Des ordinateurs, cartes à puces ou autres dispositifs qui le composent? Ce ne sont que des machines. Elles ignorent la loi. Leur vérité se trouve dans les programmes qu'elles exécutent, mécaniquement, dans la plus totale indifférence de la loi ou des conséquences sur les citoyens. Un guichet automatique ou une carte à puce ont donc leur vérité propre, qui peut très bien contredire celle du texte de loi qui leur permet d'exister ».

L'analyse rigoureuse des impacts sur la vie privée de l'introduction d'une technologie ou d'un système permettrait à un gouvernement de savoir si réellement les technologies et les systèmes qu'il acquiert et qu'il développe respectent la lettre et l'esprit des lois de protection de la vie privée.

Le gouvernement, je le comprends, veut assurer une certaine sécurité aux transactions qui sont effectuées dans le monde virtuel. Pour ce faire, il doit élaborer des politiques, puis choisir des moyens et des dispositifs de sécurité. S'ils sont bien souvent alliées, vie privée et sécurité s'affrontent parfois.

Certains dispositifs de sécurité nécessitent une cueillette supplémentaire de données personnelles, effectuent une surveillance automatique des actions posées, tracent les transactions et génèrent des fichiers sur les comportements des personnes. Une certaine réserve s'impose en la matière, les gouvernements devant choisir des moyens et des dispositifs de sécurité qui respectent les lois et réduisent au minimum la cueillette et la génération de données personnelles. Le marché offre une catégorie de produits désignés sous le vocable général de *Privacy Enhancing Technology*. Que ce soit en matière de sécurité ou pour satisfaire d'autres besoins, un gouvernement aurait tout intérêt à favoriser le développement de tels produits et à les acquérir.

PRIVACY ENHANCING TECHNOLOGY

Actuellement, quelques produits de type Privacy Enhancing Technology sont offerts sur le marché comme des logiciels permettant la navigation anonyme sur Internet ou facilitant la gestion des données personnelles. Si certains de ces produits sont reconnus comme fiables et efficaces, d'autres sont actuellement contestés par des défenseurs de la vie privée. Encore une fois une analyse rigoureuse et indépendante de ces solutions technologiques permettrait d'y voir plus clair et ce, avant toute acquisition.

CONCLUSION

La protection de la vie privée et des données personnelles ne saurait reposer simplement sur l'utilisation de technologies assurant la sécurité dans un monde virtuel. Cette protection passe plutôt par la mise en place d'un cadre législatif qui lui-même trouve sa source dans la culture et les valeurs d'une société.

Les technologies utilisées pour la prestation de services gouvernementaux devront respecter ces valeurs fondamentales. Considérant l'abondance et la complexité des technologies logicielles et matérielles offertes sur le marché, il n'est sûrement pas facile pour un gouvernement ou un État d'y voir clair. C'est pourquoi le développement et

l'utilisation de méthodes d'analyse d'impacts sur la vie privée et la protection des données personnelles me semblent plus que jamais nécessaire et ce, avant l'introduction de toute technologie et de tout système. Le développement et l'utilisation de *Privacy Enhancing Technology* semblent aussi une voie vers laquelle devrait regarder tout gouvernement soucieux de protection de la vie privée.

Quant à l'organisme sous ma responsabilité, il continuera d'être proactif, en lançant les avertissements qui s'imposent lorsque de nouvelles technologies susceptibles d'avoir des impacts sur la vie privée seront utilisées ou sur le point de l'être.

C'est ce que nous avons fait, il y a quelques mois, en réalisant une étude sur les enjeux posés par l'utilisation de la biométrie et en adoptant une série de principes d'application, dont les organismes ou les entreprises désireuses d'utiliser ces nouvelles technologies devraient tenir compte. Ces documents sont accessibles sur le site Internet de la Commission (www.cai.gouv.qc.ca).

1. Freedom of information Act and amendements of 1974 (P.L.93-501) (United States)

2. Information et liberté, Rapport de la Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels, Édition réalisée à la Direction générale des publications gouvernementales, Ministère des Communications, Gouvernement du Québec 1981, p.5

3. Un nouveau numéro d'identité accueilli par des manifestations et des boycottages, par Miwa Suzuki de l'Agence France-Presse, La Presse, 6 août 2002.

4. Japon : levée de boucliers contre le fichage numérique de la population, par Christophe Guillemin, ZDN et France, 6 août 2002.

5. Yokohama compte 3,27 millions d'habitants et est la seconde ville du Japon (www.city.yokohama.jp).

6. Japan national ID system raises privacy concers, Kuriko Miyake, IDGNews Service, Itworld.com, 8-6-02.

7. Juki Nnet goes online, Editorial, The Asahi Shimbun, Aug.6

8. La démocratie aux prises avec le gouvernement électronique, Pierrôt Péladeau, Le Devoir, 6 août 2002.

Politique de confidentialité | Copyrights